REMARKS/ARGUMENTS

Applicants appreciate the review of the present application as evidenced by the Official Action. In light of the amendments to independent claims 1, 11, 21 and 22 and the subsequent remarks, Applicants respectfully submit that the rejection of claims 1, 11, 21 and 22 under 35 USC § 102(a) as being anticipated by U.S. Patent No. 5,241,594 to Kung et al., the rejection of claims 2-4, 9, 10, 12 and 13 under 35 USC § 103(a) as being unpatentable over the Kung '594 patent in view of U.S. Patent No. 5,661,807 to Guski et al., and the rejection of claims 5-8 and 15-18 under 35 USC § 103(a) as being unpatentable over the Kung '594 patent in view of the Guski '807 patent and further in view of the Microsoft Press, Computer Dictionary, 3rd Edition are overcome and request reconsideration and allowance of the present application.

A. The Rejections under 35 U.S.C. §§ 102(a) and 103(a) are Overcome

The Official Action rejected claims 1, 11, 21 and 22 under 35 USC § 102(a) as being anticipated by U.S. Patent No. 5,241,594 to Kung et al., claims 2-4, 9, 10, 12 and 13 under 35 USC § 103(a) as being unpatentable over the Kung '594 patent in view of U.S. Patent No. 5,661,807 to Guski et al., and claims 5-8 and 15-18 under 35 USC § 103(a) as being unpatentable over the Kung '594 patent in view of the Guski '807 patent and further in view of the Microsoft Press, Computer Dictionary, 3rd Edition. As described below, however, the method, system and computer-readable medium for performing multiple user authentication with a single sign-on of the claimed invention are not taught or suggested by the the Kung '594 patent, the Guski '807 patent or the Microsoft Press, Computer Dictionary, 3rd Edition, taken either individually or in combination.

The Kung '594 patent discloses a system and method of authenticating users in a distributed computing system that includes a multiple logon procedure used in the communication protocol of the system. The user is required to log onto the distributed computing system only a single time and then the user can access all available computers connected to the network via the multiple logon procedure. Thus, when a user desires to use a particular computer, such as a remote database, for example, a request initiated by the user is processed by

the multiple logon procedure which accesses a stored file that contains the user ID codes and encrypted passwords, accesses the remote computer and then enters the user's ID code and password for that computer. The multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. See Col. 2, lines 12-50. The authentication information transmitted in the network is protected by using a secure protocol and communication path to prevent others from recording the authentication information for later logon attempts, to prevent others from impersonating another user, and to guarantee the integrity of the authentication information. See Col. 3, lines 18-24. The system and method of the Kung '594 patent requires that the computers in the distributed processing environment use substantially the same one-way encryption algorithm for encrypting passwords. An individual user is assigned a single password for the entire system 10. After the user successfully logs onto one computer, such as the workstation 11, the encrypted password is transmitted by a secure transfer protocol 22 to the remote host computer 13 where, if the received ID code and encrypted password matches the ones stored at the remote host computer 13, the user is automatically logged on. See Col. 6, lines 3-15 and Figure 1. The Kung '594 patent also states that the invention may be easily configured to work with mainframes and workstations by simply registering a user at the multiple logon server. See Col. 3, lines 35-37.

The Guski '807 patent discloses an authenticating system that uses one-time passwords. A system 100 of the Guski '807 patent includes a requesting node 102 and an authenticating node 104 interconnected by a communications channel 106. The requesting node 102, which is assumed to be a personal computer or workstation, contains a one-time password generator 300. The requesting node also has memory locations for storing a user ID 302 identifying the user, an application ID 304 identifying the host application being accessed, a signon key 306 used as a key for the encryptions and a time/date value 308. Values 302-308 provide inputs to the password generator 300. Thus, the password generator 300 generates a one-time password 310 as a function of the user ID 302, application ID 304, signon key 306 and time/date 308. Password 310 is transmitted to the authenticating node 104, together with the user ID 302 and application ID 304, as part of the signon request 320. The authenticating node 104, which is

assumed to be a host computer, contains a password evaluator 312 that receives the signon key 314 and the signon request 320 from the requesting node 102. Password evaluator 312 uses these quantities to regenerate the original time/date 308, which is compared with the reference time/date 316 to determine whether the difference between the two is within a predetermined tolerance. If so, the password evaluator 312 authenticates the user and grants access to the application; otherwise the evaluator denies access. See col. 6, line 7 to col. 7, line 1 and Figure 1.

Each one-time password that is correctly generated includes a particular "signature." The signature is exploited as a performance advantage during the one-time password evaluation process to quickly recognize (before decipherment of the password) 8-character string passwords that cannot possibly be valid one-time passwords and may therefore be trivially rejected. See col. 11, lines 40-48. Stated somewhat differently, the translation routine generates a password containing redundancy. Other means such as checksums or the like may also be used to produce an authentication code containing the desired redundancy. See col. 11, lines 49-65.

The Microsoft Press, Computer Dictionary, 3rd Edition states that a flag can be a code, embedded in data, that identifies some condition, or it can be one or more bits set internally by hardware or software to indicate an event of some type, such as an error or the result of comparing two values.

In contrast to the disclosures described above, amended independent claims 1, 11, 21 and 22 recite a method, systems and computer readable mediums for performing multiple user authentications with a single sign-on by performing a first user authentication, selecting a remote server, and sending a token to the remote server that contains authentication information responsive to the first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. The authentication information is then decoded to induce a second user authentication. Dependent claims 5, 7, 15 and 17 have also been amended to more clearly describe that the information regarding an account for the user may be a new user flag and/or user profile update information.

An example of the capability of the claimed invention to add new user accounts to the remote server is described in page 16, line 6 to page 18, line 4 of the specification and with

reference to Figure 8. In step 802, the user performs an intranet user authentication. In decision step 804, the Intranet server determines whether the user is a new user. If so, the Intranet server sets a new user flag in step 806. In step 808 the Intranet server forms the fields for the token, including the new user flag, and, in step 810, the token fields are concatenated to form a single binary string. In step 814, the binary string is encrypted. The remote server then receives and decrypts the token in step 822 and, if the remote server determines the token is valid, the new user flag status is tested in step 828. If the new user flag is set and if the remote server software is set to enable adding new users, then in step 834, the remote server tests to see if the username is already in use. If not, then, in step 838, a new user account is established, and, in step 840, the user is authenticated.

An example of the capability of the claimed invention for transmitting new or updated user profile information to the remote server is described in page 18, line 5 to page 20, line 2 of the specification with reference to Figure 9. The user profile information may include information about the user that may help the remote server provide efficient service to the user. For instance, if the remote server is a travel reservation and booking service, user profile information may include dietary choices, seating preferences, travel spending limits and other information specific to a given user. In step 902, the user performs an Intranet user authentication. In decision step 904, the Intranet server determines if the user wishes to create a new user profile or update an existing user profile. If so, the Intranet server places the user profile data into strings in step 906. In step 908, the Intranet server forms the fields for the token, including the new user profile data and, at step 910, the token fields are concatenated to form a single binary string. In step 914, the binary string is encrypted. The remote server then receives and decrypts the token in step 922 and, if the remote server determines the token is valid, the token is examined for user profile information in step 928. If user profile information is found and if the remote server software is set to enable updating user profile information, then in step 938, the remote server creates a new user profile or updates any existing user profile.

While the Kung '594 patent discloses a system and method of authenticating users in a distributed computing system that includes a multiple logon procedure used in the communication protocol of the system, it does not describe performing multiple user

authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and _information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user_, as recited by amended independent claims 1, 11, 21 and 22. The Kung '594 patent describes that when a user desires to use a particular computer, such as a remote database, for example, a request initiated by the user is processed by the multiple logon procedure which accesses a stored file that contains the user ID codes and encrypted passwords, accesses the remote computer and then enters the user's ID code and password for that computer. The multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. Thus, the Kung '594 patent does not describe any type of information that is contained in the password, _let alone information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user_, as recited by amended independent claims 1, 11, 21 and 22. Although the Kung '594 patent also states that the invention may be easily configured to work with mainframes and workstations by simply registering a user at the multiple logon server, this does not describe creation of a new user account or updating of an existing user account, it only states that once a user logs onto the multiple logon server, the user may access other remote hosts, such as mainframes and workstations, because the user ID and password stored on the multiple logon server are used to log the user onto the remote host without further input from the user.

The Guski '807 patent discloses an authenticating system that uses one-time passwords, but it does not describe performing multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and _information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user_, as recited by amended independent claims 1, 11, 21 and 22. While the Guski '807 patent states that the password generator 300 generates a one-time password 310 as a function of the user ID 302, application ID 304, signon key 306 and time/date 308, it does not state that the one-time password that is sent to an authenticating node includes any information regarding an account for the user, such as the

creation of a new user account or updating of an existing user account, as recited in the claimed invention.

Furthermore, the statements defining a flag in the Microsoft Press, Computer Dictionary, 3rd Edition also do not describe performing multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and information regarding an áccount for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by amended independent claims 1, 11, 21 and 22. Although the Microsoft Press, Computer Dictionary, 3rd Edition states that a flag can be a code, embedded in data, that identifies some condition, or it can be one or more bits set internally by hardware or software to indicate an event of some type, such as an error or the result of comparing two values, this does not teach or suggest that a token may contain information regarding an account for the user that includes a new account and/or an update to an existing account for the user, as recited in the claimed invention.
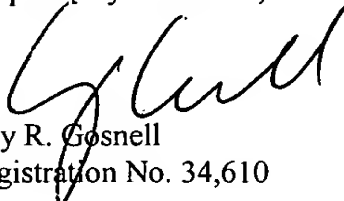
Thus, none of the disclosures of the Kung '594 patent, the Guski '807 patent or the Microsoft Press, Computer Dictionary, 3rd Edition reference, taken individually or in combination teach or suggest including information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user in a token that is sent to a remote server, as recited by amended independent claims 1, 11, 21 and 22. Since the independent claims are patentably distinct from the cited references, the claims that depend therefrom are also patentably distinct from the cited references for at least the same reasons since the dependent claims include each of the elements of a respective independent claim. Consequently, Applicants submit that, for at least those reasons set forth above, the rejections of the claims under 35 U.S.C. § 102(a) and 35 U.S.C. § 103(a) are overcome.

CONCLUSION

In view of the amendments and the remarks presented above, it is respectfully submitted that all of the present claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a Notice of Allowance be issued. The Examiner is encouraged to contact Applicants' undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.
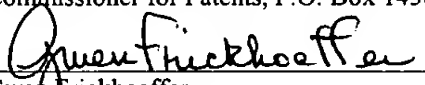
Respectfully submitted,

Guy R. Gosnell
Registration No. 34,610

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 24, 2004

Gwen Frickhoeffer

CLT01/4618450v1